UPRAVO SAM UKRAO TVOJU LOZINKU / KREDITNU KARTICU / OSOBNE PODATKE

Toni Perković

FESB, Sveučilište u Splitu, Hrvatska

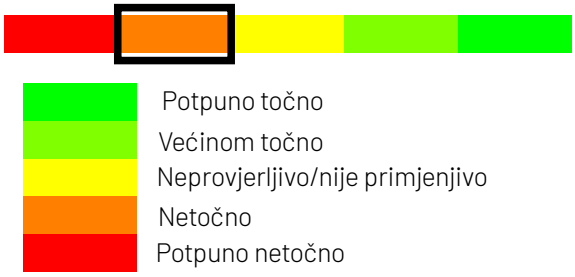
Sažetak

Phishing napadi predstavljaju značajnu prijetnju korisnicima i organizacijama u današnjem digitalnom okruženju, budući da kibernetički kriminalci neprestano razvijaju svoje tehnike kako bi iskoristili ranjivosti i pribavili osjetljive informacije. Nedavna istraživanja prikazuju različite aspekte phishinga, pružajući temeljit uvid u njegove trendove, posljedice i obrambene mehanizme. Ova studija namijenjena je donositeljima odluka, istraživačima i industrijama kao vodič za strateške odluke. Istraživanje koristi kombinaciju pregleda literature, statističke analize i studija stvarnih slučajeva kako bi se istražile tehnike i učinci phishing napada, s posebnim naglaskom na slučajeve u Hrvatskoj. Rad analizira tehnologije za otkrivanje napada, strategije podizanja svijesti korisnika te najnovije trendove, uz detaljan prikaz uloge strojnog učenja (ML) i umjetne inteligencije (AI). Osim toga, rad procjenjuje ljudske čimbenike i važnost edukativnih kampanja u osviještavanju, naglašavajući da je višeslojna obrana – koja kombinira obuku korisnika, tehnička rješenja i organizacijsku politiku – ključna za smanjenje rizika.

Ključne riječi: *Phishing napadi; Kibernetička sigurnost; Socijalni inženjering; Prijevara putem e-pošte; Kompromitacija poslovne e-pošte (BEC); Smishing; Otkrivanje phishinga*

Za upite: toperkov@fesb.hr

VJERODOSTOJNOST



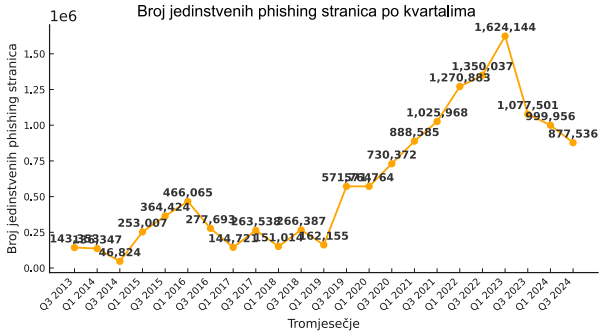
Što je phishing: Phishing je oblik internetske prijevare u kojem se napadači predstavljaju kao pouzdani subjekti kako bi prevarili žrtve da otkriju osjetljive informacije ili instaliraju zlonamjerni softver[1]. Te prijevare obično se pojavljuju putem e-pošte, SMS poruka ili telefonskih poziva i često potiču primatelja da klikne na poveznicu ili unese povjerljive podatke (kao što su lozinke, brojevi kreditnih kartica ili jednokratni kodovi). Pojam „phishing" igra se konceptom „pecanja" žrtava; a piše se s „ph" kao referenca na rane internetske „phone phreaks" – hakerske zajednice koje su istraživale telekomunikacijske sustave[2]. Prva zabilježena upotreba izraza „phishing" u ovom kontekstu datira iz 1996. godine na AOL forumu.

Podrijetlo i učinak: Phishing napadi postoje od sredine 1990-ih i izrasli su u jedan od najraširenijih oblika kibernetičkih prijetnji danas. U tipičnom phishing napadu, napadač šalje poruku koja se prikazuje kao legitimni zahtjev – primjerice, e-poruku koja izgleda kao da dolazi od vaše banke ili popularne usluge – s ciljem krađe korisničkih podataka, osobnih informacija ili novca. Budući da ti napadi iskorištavaju ljudsko povjerenje, bilo tko može postati meta: pojedinci mogu doživjeti krađu identiteta ili financijski gubitak, a organizacije mogu biti prevarene u skupe pogreške ili gubitke podataka. Phishing je izrazito čest – primjerice, najčešći je oblik kibernetičkog kriminala prijavljenog u SAD-u 2022. godine (više od 300.000 incidenata)[3]. Istraživanja u Europi također po-

[1] https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/phishing

[2] https://www.phishing.org/history-of-phishing

[3] https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics



Slika 1: Broj jedinstvenih phishing stranica po kvartalu.

kazuju da se većina organizacija susrela s phishingom. U jednoj britanskoj studiji, 79% poduzeća prijavilo je pokušaje phishinga tijekom godine, a više od polovice izjavilo je da je to bio najrazorniji oblik napada koji su doživjeli. Jasno je da phishing ima ozbiljne posljedice i za pojedince i za tvrtke, uzrokujući stvarnu financijsku štetu i rizik za privatnost.

Phishing nastavlja eskalirati kao globalna kibernetička prijetnja, o čemu svjedoči značajan porast registracija phishing domena posljednjih godina. Prema podacima portala Statista[4], broj otkrivenih phishing domena globalno je porastao s približno 75.000 u 2017. na više od 570.000 u 2023. godini. Taj eksponencijalni porast naglašava intenziviranje phishing aktivnosti, ističući prilagodljivu prirodu i skalabilnost ovih prijetnji. Budući da napadači sve više koriste registraciju domena za obmanu korisnika, ključno je da i pojedinci i organizacije budu informirani o novim phishing taktikama i proaktivni u primjeni preventivnih sigurnosnih mjera.

"broj otkrivenih phishing domena globalno je porastao s približno 75.000 u 2017. na više od 570.000 u 2023. godini"

1. Radovi na temu phishing napada

Phishing napadi u današnjem digitalnom okruženju predstavljaju značajne prijetnje korisnicima i organizacijama, budući da kibernetički kriminalci neprestano razvijaju svoje tehnike kako bi iskoristili ranjivosti i došli do osjetljivih podataka. Ti napadi obično obmanjuju žrtve da same otkriju osobne informacije, predstavljajući se kao pouzdane organizacije. Uočava se porast učestalosti ovih napada, ali i sve veća sofisticiranost u njihovoj izvedbi. Nedavne studije prikazuju različite aspekte phishinga, pružajući temeljit uvid u njegove trendove, posljedice i mehanizme obrane.

Prvo, različite tehnike koje koriste phishing napadači izazvale su veliko zanimanje akademske zajednice. Novije analize ističu kako se phishing napadi mogu klasificirati u više naprednih kategorija, uključujući ciljani phishing (spear phishing), napade "protivnika u sredini" (adversary-in-the-middle), te napade unutar preglednika (browser-in-the-browser) [1] [2]. Posebno se naglašava trend prema personaliziranim napadima koji se oslanjaju na tehnike socijalnog inženjeringa, čime se povećava njihova učinkovitost [3] [4]. Kako se metode otkrivanja tradicionalnog phishinga poboljšavaju, napadači razvijaju nove pristupe koji dodatno otežavaju obranu [1] [5].

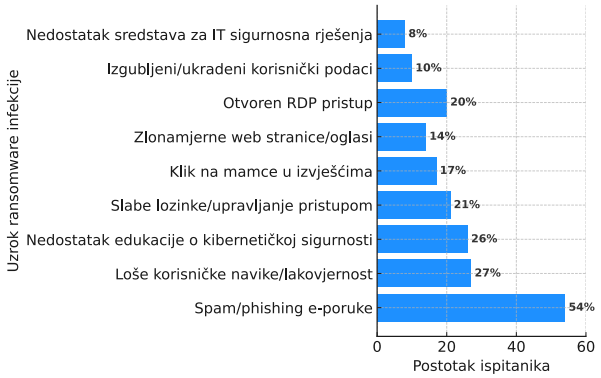
Učinci phishinga nadilaze neposredne financijske gubitke i uključuju dugoročnu štetu organizacijama, uključujući narušavanje reputacije i gubitak povjerenja korisnika [3] [6]. Istraživanja naglašavaju da osim izravnih financijskih gubitaka, organizacije snose i velike rizike povezane s narušenom sigurnošću podataka, što može destabilizirati odnose sa dionicima i smanjiti tržišnu vrijednost [7] [8]. Ti zaključci ukazuju na potrebu ne samo za reakcijom na neposredne prijetnje, već i za provedbom snažnih strategija obnavljanja povjerenja i zaštite reputacije [9] [10].

Posebna grana istraživanja usmjerena je na primjenu naprednih metoda i tehnologija za otkrivanje phishinga. Strojno učenje (Machine Learning - ML) i umjetna inteligencija (AI) istaknuli su se kao ključni alati u borbi protiv phishing napada. Nedavne studije preporučuju implementaciju modela temeljenih na dubokom učenju, kao što su rekurentne jedinice s ulaznim vratima (GRU) i konvolucijske neuronske mreže (CNN), za poboljšanje sposobnosti otkrivanja prevara[11] [12] [13]. Ovi modeli koriste bogate skupove podataka za povećanje točnosti predviđanja i smanjenje lažno pozitivnih rezultata – što je ključno za prilagodbu promjenjivoj prirodi phishing napada [12] [14].

Nadalje, sustavi za otkrivanje phishinga temeljeni na URL-u, koji primjenjuju tehnike poput logističke regresije u kombinaciji s TF-IDF analizom, sve se češće koriste za učinkovitu borbu protiv prijetnji [15] [16]. Raste broj istraživača koji naglašavaju važnost hibridnih modela koji kombiniraju više tehnika strojnog učenja kako bi se poboljšala razlika između legitimnih i zlonamjernih URL-ova [17] [18] [19]. Ovaj višeslojni pristup ne samo da povećava točnost otkrivanja, već i odgovara na stalno mijenjajuće taktike napada, koje često koriste metode prikrivanja radi izbjegavanja tradicionalnih sigurnosnih mjera [20] [21].

Ljudski faktor i dalje je ključna stavka u prevenciji phishinga. Studije pokazuju da svijest korisnika značajno utječe na njihovu ranjivost na ovakve napade, što ističe potrebu za sveobuhvatnim edukacijskim programima usmjerenima na jačanje sigurnosne svijesti [22] [23] [24]. Empirijska istraživanja sugeriraju da bi kampanje podizanja svijesti, u kombinaciji s tehnološkim rješenjima, mogle dovesti do znatnog smanjenja stope uspješnosti phishing napada, budući da poboljšavaju korisničke sposobnosti donošenja odluka u susretu s potencijalno zlonamjernim komunikacijama [23] [24].

[4] https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/



Slika 2: Phishing e-poruke uzrokuju 54% ransomware infekcija.

U području mobilne sigurnosti, phishing napadi sve se češće usmjeravaju prema korisnicima putem aplikacija poput WhatsAppa i sučelja za mobilno bankarstvo. Mobilno okruženje predstavlja posebne izazove i povećava rizike za pojedince i financijske institucije, jer napadači kreiraju poruke dizajnirane da prevare korisnika u osobnijem kontekstu [25] [19]. Istraživanja o mobilnom phishingu posebno se bave ranjivostima tih platformi, naglašavajući potrebu za prilagođenim sigurnosnim rješenjima koja odražavaju obrasce korištenja i ponašanja mobilnih korisnika [26] [25].

Dodatno, računarstvo u oblaku i druge nove tehnologije doprinose poboljšanju mogućnosti otkrivanja phishinga. Istraživanja okvira koji koriste algoritme strojnog učenja utemeljene u oblaku otvaraju potencijal za otkrivanje phishing napada u stvarnom vremenu na različitim digitalnim platformama. Novi modeli sugeriraju integraciju infrastrukture u oblaku s metodama strojnog učenja radi razvoja prilagodljivih obrana protiv phishing prijetnji, naglašavajući važnost sigurnosti oblaka u suvremenim strategijama kibernetičke sigurnosti [27] [28].

2. Nedavni pokušaji phishinga

Phishing ostaje stalna kibernetička prijetnja koja se razvija kroz nove sheme usmjerene na pojedince i organizacije (Slika 1). U nastavku su opisani ključni oblici nedavnih phishing napada:

2.1 Phishing putem e-pošte

Phishing putem e-pošte uključuje obmanjujuće poruke koje oponašaju legitimne izvore kako bi ukrale podatke ili distribuirale zlonamjerni softver. Uobičajene taktike uključuju lažna upozorenja koja primatelja potiču da verificira račun ili resetira lozinku. Te poveznice često vode do lažnih stranica koje prikupljaju pristupne podatke. Značajan primjer uključuje e-poruke koje se predstavljaju kao banke, upozoravajući na probleme s računom i nudeći poveznice prema lažnim stranicama za prijavu. Adresa pošiljatelja i sama poveznica često sadrže suptilne naznake prijevare. U 2022. godini, 91 % britanskih poduzeća prijavilo je uspješne pokušaje phishinga, uz sve veći broj slučajeva u kojima se napadači predstavljaju kao kripto ili platne usluge [5].

2.2 Phishing putem društvenih mreža

Hakeri iskorištavaju društvene mreže putem oglasa i poruka koje korisnike navode na lažne stranice, često reklamirajući izmišljene popuste ili nagradne igre[6]. Te phishing stranice oponašaju poznate brendove kako bi ukrale podatke za prijavu ili plaćanje.

Prijevare se također odvijaju putem izravnih poruka s kompromitiranih računa ili lažnih profila korisničke podrške (tzv. "angler phishing")[7]. Nova varijanta su i "deepfake" prijevare – primjerice, nedavni slučaj u kojem je korišten AI-generirani sadržaj s likom Brada Pitta kako bi se emocionalno i financijski prevarile žrtve[8,9].

2.3 Phishing za krađu vjerodajnica – Lažne web stranice

Phishing napadači često izrađuju gotovo identične stranice za prijavu za banke, e-poštu i servise u oblaku. Žrtve slijede poveznice iz e-poruka ili poruka, vjerujući da se prijavljuju na prave usluge. Primjerice, lažna e-poruka banke može voditi na stranicu poput www.banknamesecurity.com, gdje se prikupljaju korisnički podaci[10].

Takve lažne stranice postoje za mnoge usluge – Google, Microsoft, društvene mreže – stoga je važno biti iznimno oprezan. Uvijek pažljivo provjerite URL i ne klikajte na poveznice u neželjenim porukama. Krađa vjerodajnica i dalje je jedna od najraširenijih phishing taktika.

2.4 Phishing poslovnih transakcija: Prevara direktora (CEO fraud) i BEC

Tvrtke su česte mete phishing prijevara usmjerenih na financijske zlouporabe[11]. Prevara uključuje lažne, hitne zahtjeve za plaćanjem koji dolaze s kompromitiranih ili krivotvorenih e-mail adresa izvršnih, nadređenih osoba. Kompromitacija poslovne e-pošte (BEC) obično podrazumijeva manipulaciju plaćanjima faktura putem lažnog predstavljanja dobavljača.

Ovi napadi često potječu iz provaljenih e-mail računa, što ih čini vrlo uvjerljivima. U 2022. godini, gubici zbog BEC napada globalno su iznosili gotovo 2,9 milijardi američkih dolara[12]. I hrvatske tvrtke prijavile su značajne gubitke. Ključni obrambeni mehanizmi uključuju neovisnu potvrdu zahtjeva za plaćanjem putem drugog komunikacijskog kanala.

[5] https://consumer.ftc.gov/consumer-alerts/2023/05/those-urgent-emails-metamask-and-paypal-are-phishing-scams
[6] https://lifelock.norton.com/learn/fraud/facebook-scams
[7] https://www.redpoints.com/blog/social-media-phishing/
[8] https://www.mcafee.com/blogs/internet-security/brad-pitt-romance-scam-explained-how-to-prevent-scams/
[9] https://www.index.hr/magazin/clanak/predstavio-joj-se-kao-brad-pitt-i-trazio-novac-za-lijecenje-uplatila-mu-830000-eura/2632721.aspx
[10] https://total-croatia-news.com/lifestyle/internet-scams
[11] https://hoxhunt.com/guide/phishing-trends-report
[12] https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

49%	Porast phishinga od 2021.
65%	Napada usmjereni na organizacije
35%	Napada usmjereni na pojedince
90%	Zlonamjernih priloga vodi do daljnjeg socijalnog inženjeringa
0.7%-4.7%	Prijavljen phishinga koji je napisala AI

Slika 3: Razvoj phishing napada od 2021.

Slika 4: Primjer SMS phishing pokušaja.

Nedavna izvješća ukazuju na to da phishing kampanje sve češće koriste umjetnu inteligenciju za imitaciju legitimnih poruka, čime povećavaju svoju učinkovitost[13], (Slika 3). Među najčešće ciljanim sektorima nalaze se financije, tehnologija i zdravstvo, što dodatno naglašava potrebu za snažnom zaštitom i edukacijom korisnika.

2.5 SMS phishing – Smishing

Smishing koristi SMS poruke koje se predstavljaju kao legitimne usluge kako bi korisnike naveli da kliknu na zlonamjerne poveznice (Slika 2). Uobičajena prijevara tvrdi da je došlo do problema s dostavom paketa te traži uplatu naknade ili potvrdu informacija.

Na primjer, Hrvatska pošta upozorila je na lažne SMS poruke koje zahtijevaju plaćanje carine putem poveznica koje oponašaju službene stranice. Žrtve tada unose podatke s kartice koji se zatim iskorištavaju.

Ostale varijante smishinga uključuju poruke koje se predstavljaju kao banke, državna tijela ili poruke vezane za COVID-19 upute. Nikada ne klikajte na poveznice u neželjenim porukama – umjesto toga, provjerite informacije putem službenih aplikacija ili korisničke službe. SMS poruke treba tretirati s istom razinom opreza kao i e-poruke kako bi se spriječile prijevare.

3. Nedavni slučajevi u Hrvatskoj

Kao i mnoge druge zemlje, Hrvatska je posljednjih godina zabilježila nagli porast phishing incidenata koji pogađaju i pojedince i poslovne subjekte. Ministarstvo unutarnjih poslova (MUP) izvještava da su se slučajevi kibernetičkih prijevara znatno povećali. Samo u 2022. godini zabilježena su 1.864 kaznena djela iz domene kibernetičkog kriminala, što je povećanje od 19 % u odnosu na prethodnu godinu, a pričinjena je šteta u milijunima eura[14]. Phishing i internetske prijevare čine značajan dio tih incidenata. U nastavku su neki od zapaženih primjera i trendova vezanih za phishing u Hrvatskoj.

"MUP izvještava da su se slučajevi kibernetičkih prijevara znatno povećali. Samo u 2022. godini zabilježena su 1.864 kaznena djela iz domene kibernetičkog kriminala, što je povećanje od 19 % u odnosu na prethodnu godinu, a pričinjena je šteta u milijunima eura"

Lažne dostave i prijevare na oglasnicima: Kao što je ranije spomenuto, rasprostranjena prijevara cilja korisnike internetskih oglasnika poput Njuškala ili Facebook Marketplacea. Prevarant se predstavlja kao kupac zainteresiran za proizvod i tvrdi da je već angažirao dostavnu službu. Prodavatelju šalje SMS ili poruku s poveznicom za „ispis naljepnice" ili „potvrdu dostave". Ta poveznica vodi na lažnu stranicu Hrvatske pošte koja traži unos podataka s kartice (navodno radi uplate naknade ili verifikacije). U stvarnosti, riječ je o phishing zamci – jednom uneseni podaci omogućuju prevarantu krađu sredstava. Hrvatska policija posebno je upozoravala na ovaj modus operandi, jer je velik broj građana već postao žrtvom. Ključna informacija: Hrvatska pošta nikada ne traži plaćanje putem poveznice u poruci – svaki takav zahtjev je prijevara. Zahvaljujući edukativnim kampanjama, sve više korisnika prepoznaje ovu taktiku, ali i dalje ima žrtava, osobito među onima koji nisu upoznati s načinom rada poštanskih usluga.

Ciljani phishing napad na državne institucije – 2019.: U ciljanijem slučaju, hakerska skupina izvela je spear phi-

[13] https://hoxhunt.com/guide/phishing-trends-report

[14] https://total-croatia-news.com/lifestyle/internet-scams/

shing kampanju protiv hrvatskih državnih institucija[15]. E-poruke su bile oblikovane kao službene obavijesti Hrvatske pošte ili trgovačkih lanaca i upućivale su zaposlenike (službenike) da preuzmu privitak – Excel datoteku. Datoteka je sadržavala zlonamjerne makronaredbe koje bi, ako ih se aktivira, instalirale zlonamjerni softver na računalo. Kampanja je trajala od veljače do travnja 2019., a bila je posebno značajna jer je kombinirala phishing i štetni softver s ciljem špijunaže, a ne izravne krađe novca. Događaj je potaknuo hrvatske sigurnosne institucije na izdavanje upozorenja i smjernica o oprezu pri otvaranju privitaka i klikovima na neobične poveznice. Ovaj slučaj pokazuje da phishing nije prijetnja samo običnim korisnicima, već se koristi i u sofisticiranim oblicima kibernetičke špijunaže.

Bankovne i platne prijevare: Hrvatske banke i regulatorna tijela također su se susreli s phishingom u kojem korisnici primaju lažne poruke e-pošte ili SMS poruke koje izgledaju kao da dolaze od renomiranih banaka. Primjerice, u više navrata su slane poruke koje tvrde da je potrebno potvrditi podatke radi „sigurnosne nadogradnje". Korisnici koji su kliknuli na poveznicu preusmjereni su na lažnu stranicu za prijavu u banku, gdje su napadači preuzeli njihove pristupne podatke. U nekim slučajevima, napadači su zatim pokušali obaviti lažne transakcije ili su pristupili računima. Zahvaljujući Nacionalnom CERT-u (odjelu CARNET-a za kibernetičku sigurnost) i sigurnosnim timovima banaka, mnoge takve stranice – osobito one na .hr domeni – brzo su uklonjene po prijavi. Nacionalni CERT (CERT.hr) redovito potiče javnost da prijavljuje sve phishing stranice koje koriste hrvatske domene[16] kako bi ih se što prije ugasilo i upozorilo druge potencijalne žrtve.

Prijevare s humanitarnim i hitnim apelima: Phishing napadi također se koriste krinkom dobrotvornih akcija ili hitnih situacija. Nakon prirodnih katastrofa ili tijekom pandemije COVID-19, kružile su e-pošte i Facebook objave koje su tražile donacije za lažne humanitarne organizacije. U jednom slučaju, prevaranti su se predstavili kao poznata hrvatska humanitarna udruga i slali e-poštu poduzećima tražeći hitne donacije putem poveznice – koja je zapravo vodila na lažnu stranicu za unos podataka s kartice. Takve prijevare ciljaju na dobronamjernost. Hrvatska tijela i mediji pokušali su osvijestiti javnost da uvijek doniraju isključivo putem službenih i provjerenih kanala – poput verificiranih bankovnih računa ili službenih web stranica – a ne impulzivno na temelju e-poruka ili objava.

Općenito gledajući, hrvatsko iskustvo s phishingom odražava globalne trendove: smishing (SMS phishing), osobito kroz dostavne prijevare, izrazito je rasprostranjen. Kompromitacija poslovne e-pošte pogodila je neke tvrtke; a ciljani phishing u kombinaciji s zlonamjernim softverom predstavlja prijetnju institucijama. Dobra vijest je da svijest javnosti raste. Nacionalni CERT i policija redovito objavljuju upozorenja i savjete na hrvatskom jeziku kako bi korisnicima pomogli prepoznati pokušaje prijevara. Primjerice, kampanja CERT.hr-a "Veliki hrvatski naivci" prikazala je stvarne priče žrtava i istaknula koji su se znakovi upozorenja propustili.[17]. Cilj ovih napora je preokrenuti trend obrazovanjem korisnika – jer, iako se napadači usavršavaju, informirani korisnik mnogo je otporniji na prijevaru.

4. Preporuke za svijest i prevenciju

Phishing napadi iskorištavaju ljudski faktor, stoga su edukacija i oprez najbolja obrana. Pojedinci i organizacije mogu poduzeti konkretne korake kako bi prepoznali pokušaje phishinga i izbjegli da postanu žrtve. U nastavku slijede ključne preporuke, temeljene na savjetima stručnjaka za kibernetičku sigurnost i službenih izvora poput CERT-a Hrvatske i europskih agencija.

Be suspicious of unsolicited requests: Uvijek pažljivo pregledajte e-poruke ili poruke koje traže osobne podatke, lozinke ili plaćanja, osobito ako su neočekivane. Phishing poruke često koriste hitan ili zastrašujući ton – npr. „Potrebna je hitna radnja!" ili „Vaš račun će biti zatvoren danas!" – kako bi vas prisilili na reakciju[18]. Udahnite i ne žurite s odlukom. Ako se nešto predstavlja kao iznimno hitno ili tajno, to je znak da trebate biti dodatno oprezni.

Pažljivo provjerite pošiljatelja i poveznice: Provjerite e-mail adresu pošiljatelja ili broj pošiljatelja SMS poruke. Mnoge phishing poruke dolaze s adresa koje na prvi pogled izgledaju legitimno, ali sadrže sitne greške ili neobične domene (npr. support@micros0ft.com s nulom umjesto slova "o", ili SMS s nepoznatog broja koji se predstavlja kao poznata tvrtka). Ne klikajte odmah na poveznice. Na računalu zadržite miša iznad poveznice, a na mobitelu je pritisnite i zadržite kako biste vidjeli kamo vodi. Provjerite je li to službena adresa. Napadači često koriste adrese koje su slične originalu, ali s dodatnim riječima ili tipfelerima[19]. Ako e-mail tvrdi da dolazi od vaše banke, a poveznica ne vodi na "...nazivbanke.hr", nemojte je otvarati.

Nikada ne dijelite osjetljive podatke putem e-pošte ili poruka: Legitimne institucije (banke, državna tijela, poznate tvrtke) nikada neće tražiti da im šaljete lozinke, brojeve kreditnih kartica ili jednokratne kodove putem e-maila ili SMS-a. Ako dobijete takvu poruku, gotovo sigurno je riječ o prijevari. Ne odgovarajte na takve poruke. Banka vas, primjerice, neće neočekivano kontaktirati kako bi tražila da „potvrdite PIN bankomata" ili da unesete broj kartice putem poveznice. Ako niste sigurni, kontaktirajte instituciju izravno putem službenih kanala.

Potvrdite poruke putem službenih izvora: Ako poruka tvrdi da dolazi iz tvrtke i odnosi se na vaš račun, nemojte koristiti podatke za kontakt ili poveznice unutar same poruke. Umjesto toga, sami pronađite službenu web stra-

[15] https://kratikal.com/blog/croatian-government-attacked-spear-phishing/
[16] https://www.cert.hr/savjeti/
[17] https://www.cert.hr/HrNaiva
[18] https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing
[19] https://dnevnik.hr/vijesti/hrvatska/foto-hrvatska-posta-poslala-upozorenje-prevaranti-imaju-novu-taktiku—874915.html

nicu ili broj telefona. Na primjer, ako dobijete poruku "Plaćanje nije uspjelo, kliknite ovdje", posjetite službenu stranicu tvrtke tako da ručno upišete adresu ili nazovete broj s poleđine vaše bankovne kartice[20]. Tako uspostavljate kontakt putem provjerenog kanala. Ako poruka izgleda stvarno, ali dolazi iz sumnjivog izvora – uvijek je bolje provjeriti putem poznatih podataka.

Zaštitite svoje uređaje i račune: Dobra sigurnosna praksa čini vas manje ranjivima na phishing i može umanjiti štetu ako postanete žrtva. Koristite ažurirani antivirusni softver i uključite automatska ažuriranja na računalu i mobitelu. Moderni preglednici i e-mail sustavi često upozoravaju kada pokušavate posjetiti poznatu phishing stranicu ili blokiraju zlonamjerne poruke – ali ti alati najbolje funkcioniraju kad su ažurirani. Uključite višefaktorsku autentifikaciju (MFA) na važnim računima. To znači da napadač, čak i ako ukrade vašu lozinku, neće moći pristupiti računu bez dodatnog koda (npr. s vašeg mobitela). MFA je jedna od najučinkovitijih obrana. Također, redovito izrađujte sigurnosne kopije važnih podataka (lokalno ili u oblaku) – to vas neće zaštititi od phishinga, ali može pomoći ako phishing e-poruka sadrži ransomware (vrsta štetnog softvera koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za uklanjanje ograničenja).

Naučite prepoznavati znakove phishinga i educirajte druge: Phishing e-poruke često sadrže prepoznatljive znakove prijevare, poput općih oslovljavanja („Poštovani korisniče"), loše gramatike, tipfelera ili nesklada u sadržaju (npr. e-mail o bankovnom računu koji nemate). Nacionalni CERT-i i organizacije za kibernetičku sigurnost objavljuju primjere i kontrolne liste. Primjerice, CERT.hr ima infografike sa šest savjeta za prepoznavanje lažnih poruka, koje uključuju provjeru pošiljatelja, traženje gramatičkih pogrešaka i oprez pri porukama koje zvuče „predobro da bi bile istinite". Organizacijama se preporučuje redovita edukacija zaposlenika o phishingu. Mnoge velike povrede sigurnosti počele su klikom zaposlenika na phishing poruku. Edukacija zaposlenika jednako je važna kao i tehnička zaštita. Simulacije phishing napada i obnavljanje znanja o novim trendovima (npr. smishing ili prijevare povezane s COVID-19) održavaju razinu svijesti. Europska agencija za kibernetičku sigurnost (ENISA) i nacionalni CERT-i svake godine u listopadu nude besplatne materijale u sklopu Europskog mjeseca kibernetičke sigurnosti.

Uvedite pravila za provjeru, osobito kod financijskih zahtjeva: Ovo se posebno odnosi na organizacije, ali vrijedi i za privatne situacije. Uspostavite jasan protokol za potvrdu svakog zahtjeva koji uključuje slanje novca ili osjetljivih podataka. Ako „izvršni direktor" e-mailom zatraži prijenos 50.000 eura, tvrtka bi trebala imati pravilo da se svaki takav zahtjev potvrdi telefonski ili osobno. Mnoge organizacije koriste jednostavno pravilo: nema transfera samo na temelju e-maila. I privatni korisnici trebali bi provjeravati sumnjive račune ili podatke – jeste li očekivali taj račun? Je li broj računa isti kao prije? E-mail adrese mogu biti lažirane, a računi provaljeni – ono što stoji u polju pošiljatelja nije dokaz autentičnosti. Brza potvrda putem drugog kanala može spriječiti prijevaru.

Slijedite službene smjernice i prijavite incidente: Nacionalne institucije redovito objavljuju upozorenja o aktualnim phishing kampanjama (npr. CERT Croatia redovno obavještava o phishing kampanjama koje ciljaju hrvatske korisnike). Informiranost putem pouzdanih izvora (bilteni CERT-a, Europol, Interpol, agencije za zaštitu potrošača) pomaže da ostanete u tijeku s novim oblicima prijevara (npr. lažne poruke o povratu poreza ili dostavi). Ako primijetite phishing pokušaj – prijavite ga. U Hrvatskoj, e-poruku možete proslijediti Nacionalnom CERT-u, posebno ako phishing stranica koristi .hr domenu ili se odnosi na domaću tvrtku. Oni mogu pomoći ukloniti lažnu stranicu i upozoriti javnost. Također, phishing poruke možete prijaviti organizaciji koju napadači oponašaju (banke, pošte, servisi) ili međunarodnim antiphishing grupama. Prijava pomaže drugima, a u nekim slučajevima može dovesti i do kažnjavanja počinitelja. Ako shvatite da ste postali žrtva phishinga – odmah kontaktirajte svoju banku da blokira karticu, promijenite lozinke s pouzdanog uređaja i obratite se službenim institucijama za pomoć. Brza reakcija može značajno umanjiti štetu.

Ako slijedite ove preporuke i ostanete oprezni, znatno ćete smanjiti rizik od phishinga. Svijest je vaša najbolja obrana: kada znate da kriminalci „pecaju" korisnike, manja je šansa da ćete „zagristi udicu". Kao što često upozorava hrvatski CERT – „Razmisli prije nego klikneš" – neka nam to bude navika u današnjem digitalnom svijetu prepunom zamki.

Literatura

[1] F. Putra, U. Ubaidi, A. Zulfikri, G. Arifin, R. Ilhamsyah, "Analysis of phishing attack trends, impacts and prevention methods: literature study", Brilliance Research of Artificial Intelligence, vol. 4, no. 1, p. 413-421, 2024. https://doi.org/10.47709/brilliance.v4i1.4357

[2] E. Blancaflor, "Advanced phishing techniques: analyzing adversary-in-the-middle and browser-in-the-browser attacks in modern cybersecurity", Cybernetics and Information Technologies, vol. 25, no. 1, p. 55-77, 2025. https://doi.org/10.2478/cait-2025-0004

[3] A. -, M. Amin, L. -, A. -, R. -, R. -et al., "Understanding the impact of phishing attacks on organizational security and trust", International Journal for Multidisciplinary Research, vol. 6, no. 6, 2024. https://doi.org/10.36948/ijfmr.2024.v06i06.34230

[4] F. Jimmy, "Phishing attackers: prevention and response strategies", JAIGS, vol. 2, no. 1, p. 307-318, 2024. https://doi.org/10.60087/jaigs.v2i1.249

[5] A. Mustafa, B. PN, N. Divyashree, I. Fathima, J. Fathima, "A comprehensive review of phishing attacks techniques, types and solutions", JoHTDCPCV, vol. 1, no. 1, p. 15-24, 2024. https://doi.org/10.46610/johtdcpcv.2024.v01i01.002

[20] https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

[6] S. Chowdhary, P. Kumar, R. Mittal, I. Gumber, V. Jangra, P. Srivastava, "Phishing detection tool for financial emails", International Journal of Financial Engineering, vol. 11, no. 04, 2024. https://doi.org/10.1142/s2424786324420027

[7] D. Ogonji, W. Cheruiyot, P. Mwangi, "Hybrid phishing detecting with recommendation decision trees", International Journal of Recent Technology and Engineering, vol. 13, no. 2, p. 32-35, 2024. https://doi.org/10.35940/ijrte.b8120.13020724

[8] J. DIAS, R. Farina, F. Florian, "Segurança cibernética - estudo das técnicas de ataques cibernéticos (phishing, ransmware, ddos) de engenharia social e medidas de prevenção", Revista Científica Semana Acadêmica, vol. 12, no. 248, p. 1-16, 2024. https://doi.org/10.35265/2236-6717-248-13011

[9] A. ANDRIU, "Adaptive phishing detection: harnessing the power of artificial intelligence for enhanced email security", Romanian Cyber Security Journal, vol. 5, no. 1, p. 3-9, 2023. https://doi.org/10.54851/v5i1y202301

[10] A. Mahmood, V. Pandey, R. Raj, G. Mishra, "Detection of phishing sites using machine learning techniques", Int Res J Adv Engg Hub, vol. 2, no. 02, p. 210-219, 2024. https://doi.org/10.47392/irjaeh.2024.0034

[11] , "Phishing website detection using machine learning and deep learning techniques", pst, vol. 49, no. 1, p. 947-959, 2025. https://doi.org/10.52783/pst.1643

[12] H. Alsubaie, R. Althomali, S. Alajmani, "Deep learning approach for detection of phishing attack to strengthen network security", International Journal of Network Security Its Applications, vol. 16, no. 6, p. 01-19, 2024. https://doi.org/10.5121/ijnsa.2024.16601

[13] Z. Alshingiti, R. Alaqel, J. Al-Muhtadi, E. Qazi, K. Saleem, M. Faheem, "A deep learning-based phishing detection system using cnn, lstm, and lstm-cnn", Electronics, vol. 12, no. 1, p. 232, 2023. https://doi.org/10.3390/electronics12010232

[14] F. Alsubaei, A. Almazroi, N. Ayub, "Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics", Ieee Access, vol. 12, p. 8373-8389, 2024. https://doi.org/10.1109/access.2024.3351946

[15] M. Sibhathallah and S. -, "Detection of phishing urls using a term frequency inverse document frequency (tf-idf).", International Journal for Multidisciplinary Research, vol. 6, no. 3, 2024. https://doi.org/10.36948/ijfmr.2024.v06i03.21435

[16] M. T., M. M, S. Vigila, "Url based phishing detection", International Scientific Journal of Engineering and Management, vol. 04, no. 01, p. 1-6, 2025. https://doi.org/10.55041/isjem02220

[17] M. Gawade, "Cyber protect: a robust cybersecurity system for fraudulent scam and phishing detection using machine learning techniques", International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 11, p. 2480-2487, 2023. https://doi.org/10.22214/ijraset.2023.57066

[18] R. Abdillah, Z. Shukur, M. Mohd, T. Murah, I. Oh, K. Yim, "Performance evaluation of phishing classification techniques on various data sources and schemes", Ieee Access, vol. 11, p. 38721-38738, 2023. https://doi.org/10.1109/access.2022.3225971

[19] U. Umoga, E. Sodiya, O. Amoo, A. Atadoga, "A critical review of emerging cybersecurity threats in financial technologies", International Journal of Science and Research Archive, vol. 11, no. 1, p. 1810-1817, 2024. https://doi.org/10.30574/ijsra.2024.11.1.0284

[20] P. Kyaw, J. Gutiérrez, A. Ghobakhlou, "A systematic review of deep learning techniques for phishing email detection", Electronics, vol. 13, no. 19, p. 3823, 2024. https://doi.org/10.3390/electronics13193823

[21] O. Osliak, A. Saracino, F. Martinelli, P. Mori, "Cyber threat intelligence for critical infrastructure security", Concurrency and Computation Practice and Experience, vol. 35, no. 23, 2023. https://doi.org/10.1002/cpe.7759

[22] Y. Lee, C. Gan, T. Liew, "Thwarting instant messaging phishing attacks: the role of self-efficacy and the mediating effect of attitude towards online sharing of personal information", International Journal of Environmental Research and Public Health, vol. 20, no. 4, p. 3514, 2023. https://doi.org/10.3390/ijerph20043514

[23] S. Zhuo, R. Biddle, Y. Koh, D. Lottridge, G. Russello, "Sok: human-centered phishing susceptibility", Acm Transactions on Privacy and Security, vol. 26, no. 3, p. 1-27, 2023. https://doi.org/10.1145/3575797

[24] C. Ismiati, M. Borman, G. Putro, "Legal literacy: the role of housewives in overcoming phising criminal", Sang Pencerah Jurnal Ilmiah Universitas Muhammadiyah Buton, vol. 10, no. 2, p. 321-332, 2024. https://doi.org/10.35326/pencerah.v10i2.5075

[25] C. Mutia and R. Firdaus, "Analisis penipuan digital teknik phishing terhadap layanan mobile banking", JUTRABIDI, vol. 1, no. 4, p. 05-10, 2024. https://doi.org/10.61132/jutrabidi.v1i4.191

[26] M. Kumari, C. Priya, G. Bhavya, H. Neha, M. Awasthi, S. Tripathi, "Viable detection of url phishing using machine learning approach", E3s Web of Conferences, vol. 430, p. 01037, 2023. https://doi.org/10.1051/e3sconf/202343001037

[27] L. Abdulrahman, S. Ahmed, Z. Rashid, Y. Jghef, T. Ghazi, U. Jader, "Web phishing detection using web crawling, cloud infrastructure and deep learning framework", Journal of Applied Science and Technology Trends, vol. 4, no. 01, p. 54-71, 2023. https://doi.org/10.38094/jastt401144

[28] R. Karthika, C. Valliyammai, M. Naveena, "Phish block: a blockchain framework for phish detection in cloud", Computer Systems Science and Engineering, vol. 44, no. 1, p. 777-795, 2023. https://doi.org/10.32604/csse.2023.024086

Kutak za medije/Informacije

TKO? - Autor, Toni Perković, zaposlen je na Fakultetu elektrotehnike, strojarstva i brodogradnje (FESB) Sveučilišta u Splitu. Njegov znanstveni rad usmjeren je na područje kibernetičke sigurnosti, s posebnim naglaskom na phishing prijetnje, socijalni inženjering i razvoj mehanizama za detekciju i podizanje svijesti. S obzirom na obrazovanje iz računarstva, koristi interdisciplinarne pristupe za rješavanje stvarnih digitalnih prijetnji, ciljajući pritom i tehničke i ljudske ranjivosti.

GDJE? - Ovo istraživanje provodi se u Hrvatskoj, ali se bavi globalnim izazovom kibernetičke sigurnosti. Opisane prijetnje, poput phishing poruka putem e-pošte, smishinga i kompromitacije poslovne e-pošte (BEC), javljaju se u lokalnim i međunarodnim kontekstima – pogađaju pojedince, tvrtke i institucije diljem svijeta. Studija uključuje konkretne slučajeve iz Hrvatske, dok se šira analiza temelji na trendovima zabilježenima u Europi i Sjevernoj Americi.

KADA? - Ova studija prikazuje trenutno stanje phishinga kao jedne od najraširenijih kibernetičkih prijetnji, osobito od 2020. godine, uz jasno izraženo jačanje kroz 2023. i u današnje vrijeme. Rad također opisuje povijesni razvoj phishinga, od njegovih početaka sredinom 1990-ih do današnjih kampanja koje koriste umjetnu inteligenciju i visoko personalizirane taktike. Ujedno se predviđaju i buduće implikacije, s obzirom na sve sofisticiranije napade u skladu s razvojem digitalnih tehnologija i promjenom korisničkih navika.

ŠTO? - Rad nudi sveobuhvatan pregled phishinga kao oblika kibernetičkog kriminala, analizirajući njegovu evoluciju, metode i učinke na pojedince i organizacije. Razvrstava različite vrste phishinga – uključujući prijevare putem e-pošte, krađu vjerodajnica putem lažnih stranica, obmane na društvenim mrežama, SMS smishing i poslovne prijevare. Također se analizira tehnološka obrana (detekcija), obrazovni pristupi i najnoviji phishing trendovi, s posebnim osvrtom na Hrvatsku kao reprezentativan nacionalni primjer.

ZAŠTO I KAKO? - Motivacija iza ovog istraživanja proizlazi iz sve većeg stupnja sofisticiranosti i štetnosti phishing napada na digitalnu sigurnost, privatnost i financijski integritet. Kako bi se suočilo s tim izazovima, rad kombinira analizu stvarnih slučajeva napada (ovdje), literaturu o alatima za detekciju temeljenim na strojnom učenju (ovdje), i strategije obrazovanja korisnika. Istražuje se kako se umjetna inteligencija koristi i u napadačke i u obrambene svrhe. Nadalje, naglasak je na obrazovnim kampanjama i institucionalnim politikama kao ključnim slojevima obrane. Ovaj interdisciplinarni pristup daje uvid u načine na koje društvo može razviti otpornost na phishing – kroz osnaživanje korisnika, napredna tehnička rješenja i strateške sigurnosne politike.

Kontakt za medije

Ime i prezime: Toni Perković

E-mail: *toperkov@fesb.hr*